Inappropriate Personal Use of the Internet Jeopardizes the Security and Privacy of Taxpayer Data

June 2003

Reference Number: 2003-20-133

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

INSPECTOR GENERAL
for TAX
ADMINISTRATION

June 16, 2003

MEMORANDUM FOR ACTING CHIEF INFORMATION OFFICER

Gordon C. Milbourn III

FROM: Gordon C. Milbourn III
Acting Deputy Inspector General for Audit

SUBJECT: Final Audit Report - Inappropriate Personal Use of the Internet Jeopardizes the Security and Privacy of Taxpayer Data (Audit # 200320007)

This report presents the results of our review of personal use of the Internet by Internal Revenue Service (IRS) employees. The overall objective of this review was to evaluate employee compliance with the IRS' Internet usage policy, which was implemented in May 2002.

The IRS' Internet usage policy permits employees to use Federal Government computers to access the Internet for limited personal reasons as long as the use involves minimal costs. Personal use is permitted during both work and nonwork time for a reasonable duration and frequency of use. The policy provides a list of inappropriate personal uses.

In summary, although the policy is comprehensive and was widely distributed, a substantial number of IRS employees continued to access prohibited sites that put IRS computer systems at risk. During a 1-week period almost 6 months after the policy was implemented, IRS employees accessed over 1 million questionable web site objects from over 19,000 computer addresses. These accesses were to seven categories of sites specifically listed in the IRS policy as inappropriate: sexually explicit web sites, personal email accounts, chat rooms, games, music, instant messaging, and sites from which programs were downloaded. Because of the manner in which the IRS assigns computer addresses and because we had no means to identify all inappropriate sites, we could not determine the exact number of employees who did not comply with the policy. However, the magnitude of the results clearly indicates significant misuse of the Internet in the IRS.

Inappropriate use of the Internet can create unnecessary security risks and result in denial of service for work-related actions. Other adverse effects include productivity losses and increased telecommunications costs. Further, by allowing access to sexually explicit sites, the IRS could be accused of fostering a hostile work environment that could lead to damages and legal costs.

The IRS established a multifaceted process to monitor compliance with its Internet usage policy. Specifically, it published the policy and distributed it to all employees. Vendor software was also purchased to block employee access to certain categories of web sites. In addition, the IRS conducted limited monitoring to identify inappropriate accesses that had avoided the blocking software. However, these actions were not completely effective.

To improve IRS employee compliance with the Internet usage policy, we recommended IRS management require employees to annually document their understanding of the policy, improve site blocking and monitoring controls, and develop a strategy for publicizing Internet abuses to deter future Internet policy violations. We also recommended that the IRS assign sufficient resources for employee Internet monitoring.

Management's Response: The Acting Deputy Commissioner for Modernization & Chief Information Officer concurred with our recommendations. Actions planned or already taken include developing a communications strategy (including annual training) to enhance employees' awareness of the security risks inherent when the Internet is misused, improving content-filtering technology to block employee access to inappropriate sites, assigning responsibility for monitoring employees' Internet use, hiring a dedicated program manager to manage the program, and evaluating the use of already available scripts to identify employee misuse of the Internet. Management's complete response to the draft report is included as Appendix IV.

Office of Audit Comment: In his response, the Acting Deputy Commissioner for Modernization and Chief Information Officer questioned our approach for counting potential violations because we identified potentially inappropriate web site objects. He stated that if a web site contained 100 objects, then conceivably we would have counted 100 objects as potentially inappropriate when an employee accessed that web site. He further provided hypothetical examples of objects that we may have identified as inappropriate sites just by visiting *The Washington Post* home page and Congressional web sites.

While web sites can contain multiple objects (e.g., recent tests of the CNN and Yahoo web sites identified 81 and 18 objects, respectively), we would not have identified an object unless the object's web address contained a key word indicating it may be inappropriate. In any event, the occurrences in our results of potentially inappropriate objects on *The Washington Post* home page or Congressional web sites were extremely minimal. Only 21 of the 142,359 potentially inappropriate sexually explicit objects were accessed via *The Washington Post* web site, and only 8 of the 373,281 chat room objects we identified were accessed from Congressional web sites.

We are also certain that we did not identify all inappropriate accesses. As we pointed out in the report, our tests could not be precise due to the mechanics of the Internet. Overall, we used essentially the same methodology to identify misuse that most content-filtering software packages use in blocking sites.

Our intention in citing the total number of potentially inappropriate objects accessed was to emphasize that misuse of the Internet by IRS employees continues to be significant and widespread. Our audit emphasis was not focused on merely demonstrating the volume, especially a precise number, of policy violations. Instead, our results indicate that the relative size of the problem is still significant, and that the IRS should have been in the position to identify and monitor the problem and to initiate appropriate corrective actions, particularly since this is our second report on Internet use.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Margaret E. Begg, Acting Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

Table of Contents

Background

In May 2002, the Internal Revenue Service (IRS) implemented an Internet usage policy for its employees. The policy allows employees to use Federal Government computers for limited personal use when such use involves minimal additional expense to the Government and does not overburden any of the IRS' information resources. The policy states that limited personal use of the Internet should not affect the performance of official duties, interfere with the mission or operations of the IRS, or violate Federal Government ethical standards. Personal use is permitted during both work and nonwork time for a reasonable duration and frequency of use.

The policy was developed because of the expansion of information technology to an ever-increasing number of IRS employees, the issuance of Treasury Directive 87-04, "Personal Use of Government Office Equipment Including Information Technology," and the desire of the IRS to enhance the quality of the workplace. The policy also addresses issues in the Treasury Inspector General for Tax Administration's (TIGTA) report entitled, *Employees' Extensive Personal Use of the Internet Should Be Controlled* (Reference Number 2001-20-016, dated November 2000). In that report, we discussed that the IRS' Internet usage policy prohibited any personal use of the Internet but that there was, nevertheless, substantial nonbusiness use of the Internet by IRS employees.

This review was conducted from October 2002 to January 2003, primarily within the Office of Security Services at the IRS National Headquarters in Washington, D.C., in accordance with *Government Auditing Standards*. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

The Internet Usage Policy Is Comprehensive and Procedures Were Developed to Enforce the Policy

The IRS' policy for employee Internet use clearly and comprehensively states the IRS' position. The policy includes an appendix that lists inappropriate personal uses. It also describes sanctions for the misuse of information technology equipment and resources.

The IRS distributed the policy in an information package to all employees in May 2002. The package was accompanied by an IRS organization-wide media campaign that included a personal message from the Deputy Commissioner. An extensive Intranet web site provided additional clarification regarding access to certain categories of web sites.

Blocking software was used to prevent access to certain web sites. A web-monitoring process was implemented to identify accesses to inappropriate sites that had avoided the blocking software. In addition, the TIGTA Office of Investigations developed software that analyzes Internet logs to identify workstations accessing sexually explicit and gambling sites.

Some Employees Continued to Make Inappropriate Personal Use of the Internet

Employee abuse of the Internet is still widespread. During the week beginning October 20, 2002, over 1 million accesses[1] to web site objects[2] that were likely to be prohibited were made from over 19,000 computer addresses. Some employees continued to access sexually explicit materials, as well as personal email accounts, streaming news, music, and video sites. They downloaded games, music, videos, and other large files.

Inappropriate use of the Internet can create unnecessary security risks and result in denials of service. Organizations the size of the IRS have incurred system restoration costs and productivity losses of up to $11.5 million annually to recover from these security incidents.

Employees who access their personal email accounts via the Internet and those who access other inappropriate sites circumvent the controls designed to protect IRS computer systems. For example, work-related and personal emails sent to IRS employee accounts are screened for viruses and other malicious programs before entering the IRS network. However, emails accessed from personal email accounts via the Internet are not screened prior to entering the network.

[1] IRS employees made 1,067,556 accesses to web objects that were potentially inappropriate. A web page usually contains multiple objects. For example, recent tests of the CNN and Yahoo home pages showed they contained 81 and 18 objects, respectively.

[2] When Internet users access a web site, they are actually downloading images from the web site server. These images, which can be in the form of a picture, text document, or advertising banner, were captured as web site ***objects*** in our population.

Inappropriate use of the Internet could also result in productivity losses and increased costs to purchase enough telecommunications capacity to handle unnecessary traffic, particularly from streaming video and audio. Access to sexually explicit and other sites with inappropriate content can foster hostile work environments that could put the IRS at risk of legal actions and costs.

To make our assessment, we looked for key words in web site titles for seven categories considered inappropriate by the IRS' policy: sexually explicit web sites, personal email accounts, chat rooms, games, music, programs (i.e., downloading unauthorized software), and instant messaging. For example, we searched firewall logs to identify sites that included the key word *"chat"* in their title to identify chat rooms accessed by IRS employees.

We recognize that some of these sites may have been accessed for legitimate business reasons. However, we judgmentally tested 283 of the sites and determined that most were obviously inappropriate. The sites we tested were accessed from over 6,000 of the 19,000 computer addresses that had accessed potentially inappropriate sites.

We could not determine the exact number of employees making the accesses. Because of how the IRS assigns computer addresses, a computer could have had more than 1 address during our 1-week test. It is also possible that one employee could have accessed more than one computer during our sample. Conversely, more than one employee could have used the same computer to access the Internet. The time lag in receiving and reviewing the data also hindered our ability to calculate the number of employees misusing the Internet.

We are confident, however, that the number of employees misusing the Internet and the amount of the misuse is significant. The following chart illustrates the activity for our test week:

Prohibited Category	Total Computer Addresses	Total Objects Accessed
Chat Rooms	8,231	373,281
Games	9,338	294,619
Personal Email	10,494	170,431
Sexually Explicit	8,204	142,359
Music	5,892	54,727
Programs	4,602	22,747
Instant Messaging	124	9,392
Totals	19,581*****	1,067,556******

Source: IRS firewall logs for week of October 20, 2002.

***** Total adjusted to reflect that some computers were used to access more than one prohibited category. During the week of our review, 56,085 IRS unique computer addresses were used to access the Internet, of which 19,581 unique computer addresses were likely to have accessed inappropriate sites.

****** During the week of our review, IRS employees made over 79,574,412 accesses to web objects, of which 1,067,556 were accesses to sites likely to be inappropriate.

Although a large number of employees accessed sites likely to be inappropriate, a relatively small number of employees appear to be chronic abusers. More than 300,000 (over 28 percent) of the potentially inappropriate accesses made in the 1-week period were made from 122 computer addresses.

Employees were able to continue violating the Internet usage policy because:

- Efforts made to maintain employee awareness of the policy were not sufficient.
- Blocking software was not effective or fully used.
- The monitoring of Internet use was not effective.

Efforts made to maintain employee awareness of the policy were not sufficient

As previously mentioned, the IRS initiated extensive steps to ensure employees were made aware of the new policy. From our test results, it is obvious that many employees forgot, misunderstood, or ignored the policy requirements.

Since the initial distribution of the policy to all employees, little has been done to remind employees of their responsibilities for using the Internet. The IRS also has not taken the opportunity to publicize the results of any Internet monitoring activities being performed. Widespread publicity regarding the monitoring of the policy would provide a deterrent to further inappropriate use of the Internet.

IRS employees are also required to annually acknowledge their awareness of security policies by signing an Information System User Registration/Change Request (Form 5081). However, the Form 5081 does not specifically cite the IRS' Internet usage policy in the Information Systems Security Rules section. As a result, an opportunity to annually refresh employees' understanding of the policy and document their acknowledgement was missed.

Blocking software was not effective or fully used

During our 1-week test, approximately 40,000 of the over 1 million inappropriate accesses were blocked by content-filtering software. We identified 294,619 accesses to game sites, but the software blocked only 12,834. We identified 142,359 accesses to sexually explicit sites, but the software blocked only 24,610. The IRS' Computer Security Incident Response Center (CSIRC) indicated that the software had been inoperative for periods of time and had allowed prohibited traffic to bypass the filtering process during periods of high activity. The CSIRC indicated that it was working with the vendor to resolve these problems.

Also, at the time of our review, the software's access-blocking capabilities were not in full use. The software was not set to block accesses to chat rooms, music sites, or streaming audio or video media, even though those categories are expressly prohibited by the Internet usage policy.

The monitoring of employee Internet use was not effective

Much of the inappropriate activity identified in our review was not identified by the CSIRC. We matched our results of the top five potential violators for each of our seven categories with the CSIRC's incident reports for the same time period. Only 7 of the 35 computer addresses with the most inappropriate accesses were identified by the CSIRC.

The CSIRC indicated that resources were not always available for this monitoring due to other incident response priorities. The CSIRC has primary responsibility over intrusion detection, firewall administration, computer forensics, and incident response.

Records indicate only 126 employees were identified for disciplinary actions due to Internet abuses from May 2002 to January 2003. Eighteen cases are still open and 108 cases have been closed. Actions were taken on almost 90 percent of the cases, with dispositions including employee suspension and removal. We did not review case files to evaluate the appropriateness of actions taken. However, it appears that when cases were forwarded to IRS management, actions were taken.

The TIGTA Office of Investigations also monitors Internet usage with an automated software program it developed. This software is used for tracking the top 20 daily computer address policy violations for sexually explicit and gambling accesses. The Office of Investigations was primarily interested in these two categories because the accesses could be criminal violations. The software identified 60 percent of the same computers accessing sexual content that we identified and some additional potential computer violations that we did not identify. We attribute the disparities in identifying the computer address violations to differences in the key word criteria used to identify abuses.

To improve the IRS' process for identifying and referring violations of the policy, we believe that the Office of Investigations program for dealing with sexually explicit and gambling accesses could be merged with our strategy for identifying and categorizing other types of abuses. The

IRS' use of the modified software could improve its identification of abuses and reduce monitoring costs.

Recommendations

To resolve the identified issues, the Deputy Commissioner for Modernization & Chief Information Officer should:

1. Include the Internet usage policy as part of the annual security awareness process, which requires employees to sign Forms 5081 acknowledging that they are aware of their security responsibilities, or require employees with access to IRS computers to sign statements that they have read and understand the policy provisions.

<u>Management's Response</u>: Management added the Internet usage policy into this year's annual security training. Although management did not commit to including this issue on Form 5081, the annual security training should be adequate.

2. Resolve the deficiencies with the current blocking software, or replace it with more effective content-filtering technology, and use it to prevent accesses to a wider range of inappropriate sites.

<u>Management's Response</u>: Management has reconfigured system components and improved restrictions for known chat rooms and other high-risk sites. Actions are planned to analyze and implement a long-term content-filtering solution that dynamically updates sites that should be blocked.

3. Assign sufficient resources to monitor and analyze employee Internet usage.

<u>Management's Response</u>: Management has assigned responsibility for monitoring Internet usage under the Chief, Security Services, and authorized the hiring of a program manager to carry out these responsibilities. Responsibility for processing inappropriate Internet access activity has been centralized to ensure consistency of treatment.

4. Expand the use of existing Office of Investigations software that identifies accesses to sexually explicit and

gambling sites to the other inappropriate uses specified in the Internet usage policy.

Management's Response: Management is evaluating the existing software for identifying accesses to sexually explicit and gambling sites to determine if it can be applied to other inappropriate uses.

5. Work with the Offices of Tax Administration Coordination and Communications and Liaison to develop a strategy, which includes publicizing Internet abuses, to deter future Internet policy violations.

Management's Response: The Acting Commissioner issued a memorandum to all managers requiring them to ensure that all employees are familiar with the Internet usage policy and the potential disciplinary actions related to violations. Actions are planned to develop a comprehensive communication plan that includes multiple techniques, such as payroll stuffers, for presenting the Internet usage policy and related issues.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to evaluate employee compliance with the Internal Revenue Service's (IRS) Internet usage policy. This review is a follow-up to a previous Treasury Inspector General for Tax Administration (TIGTA) report entitled, *Employees' Extensive Personal Use of the Internet Should Be Controlled* (Reference Number 2001-20-016, dated November 2000).

I. To evaluate the processes used by the IRS to disseminate the Internet usage policy to all employees, we:

   A. Researched the IRS' Intranet web site for the current Internet usage policy, which went into effect May 13, 2002.

   B. Researched the methods the IRS used to provide employees with the policy and guidance on what usage is and is not allowed.

II. To evaluate the Internet usage policy to determine whether it adequately addresses all security risks arising from Internet accesses, we compared the Internet usage policy with Internal Revenue Manual 25.10, Treasury Directive (TD) Publications 71-10, TD 87-04, and other similar Federal Government guidelines to identify unallowable practices that are not addressed in the IRS' Internet usage policy.

III. To identify the controls and processes in place to monitor compliance with the Internet usage policy and to detect/prevent inappropriate accesses, we:

   A. Discussed with the Agency-Wide Shared Services' Personnel Services staff the role they have in investigating and monitoring Internet usage, the controls and processes that they use to monitor Internet usage, the administrative actions taken for inappropriate Internet access over the 6 months prior to the start of our review, and actions they perform to curb inappropriate accesses by employees.

   B. Discussed with the IRS' Office of Security Services staff the role they have in investigating and monitoring Internet usage, the controls and processes that they use to block or monitor inappropriate Internet usage, the actions taken when inappropriate access is identified, the actions they perform to curb inappropriate Internet accesses by employees, and whether the web-monitoring product is installed at all gateways leading to the Internet.

   C. Discussed with TIGTA Office of Investigations employees the role they have in investigating and monitoring Internet usage, the actions they perform to curb inappropriate Internet accesses by employees, and whether they investigated any inappropriate Internet usage cases in the 6 months prior to the start of our review.

IV. To determine whether there was Internet traffic to sites that are deemed inappropriate by the Internet usage policy, we:

A. Requested the firewall logs for all of the Internet gateways used by the IRS for a full week, approximately 6 months after policy went into effect. We judgmentally selected the week of October 20, 2002.

B. Retrieved the Domain Name Service (DNS)[1] tables from the Department of the Treasury or IRS Internet DNS fileservers to verify whether all of the IRS' Internet gateways listed on the DNS tables were accounted for in the firewall logs.

C. Screened the log files for seven categories of Internet web site accesses or downloads that are deemed to be inappropriate by the Internet usage policy. Judgmentally selected a total 283 sites (at least 20 from each of the 7 categories of inappropriate uses) to confirm that the sites were inappropriate. The 283 sites were visited by 6,330 computer addresses during our 1-week test period.

D. Reviewed the log files for web accesses that had been denied by the application used to stop accesses to inappropriate sites and ascertained what actions were taken by management to prevent ongoing abuses by the addresses with significant numbers of denied accesses.

E. Matched the programs downloaded from the Internet to a list of known malicious software programs based on names and file sizes.

[1] DNS is a service that translates domain (Internet site) names into their respective numeric computer addresses. Alphabetic names are easier to use than the numbers that comprise Internet addresses.

Appendix II

Major Contributors to This Report

Gary V. Hinkle, Acting Assistant Inspector General for Audit (Information Systems Programs)
Steve Mullins, Director
Leon Niemczak, Audit Manager
Richard Borst, Senior Auditor
Bret Hunter, Senior Auditor
Louis Lee, Senior Auditor
Midori Ohno, Senior Auditor
Larry Reimer, Senior Auditor

Appendix III

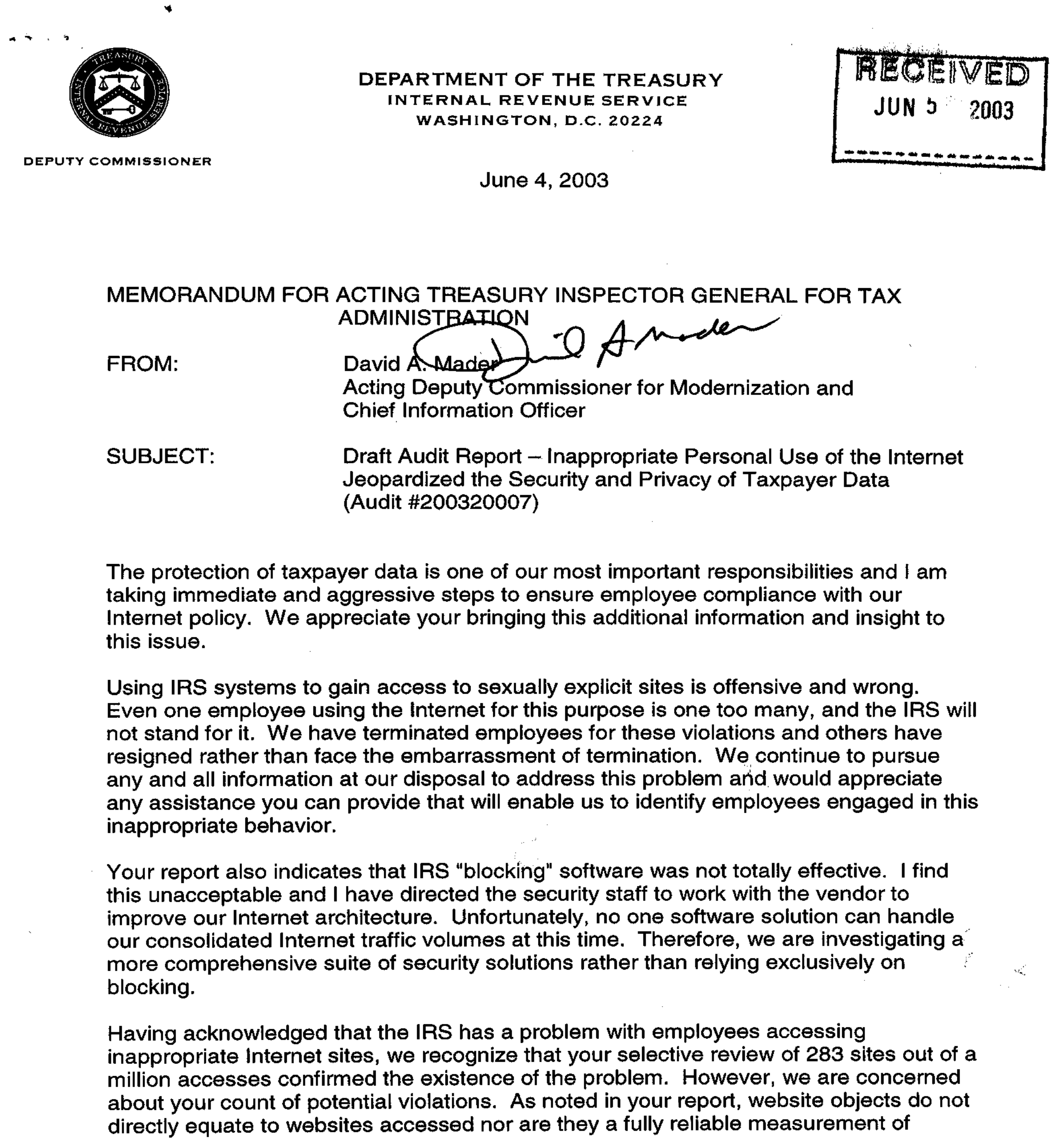
Report Distribution List

Commissioner N:C
Deputy Commissioner for Operations Support N:DC
Chief, Agency-Wide Shared Services A
Chief, Security Services M:S
Chief, Tax Administration Coordination N:ADC:T
Director, Portfolio Management M:R:PM
Director, Strategic Human Resources N:ADC:H
Chief Counsel CC
National Taxpayer Advocate TA
Director, Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis N:ADC:R:O
Office of Management and Controls N:CFO:AR:M
Audit Liaisons:

Deputy Commissioner for Modernization & Chief Information Officer M
Chief, Security Services M:S
Director, Strategic Human Resources N:ADC:H

Appendix IV

Management's Response to the Draft Report



DEPUTY COMMISSIONER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

June 4, 2003

MEMORANDUM FOR ACTING TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

FROM: David A. Mader
Acting Deputy Commissioner for Modernization and
Chief Information Officer

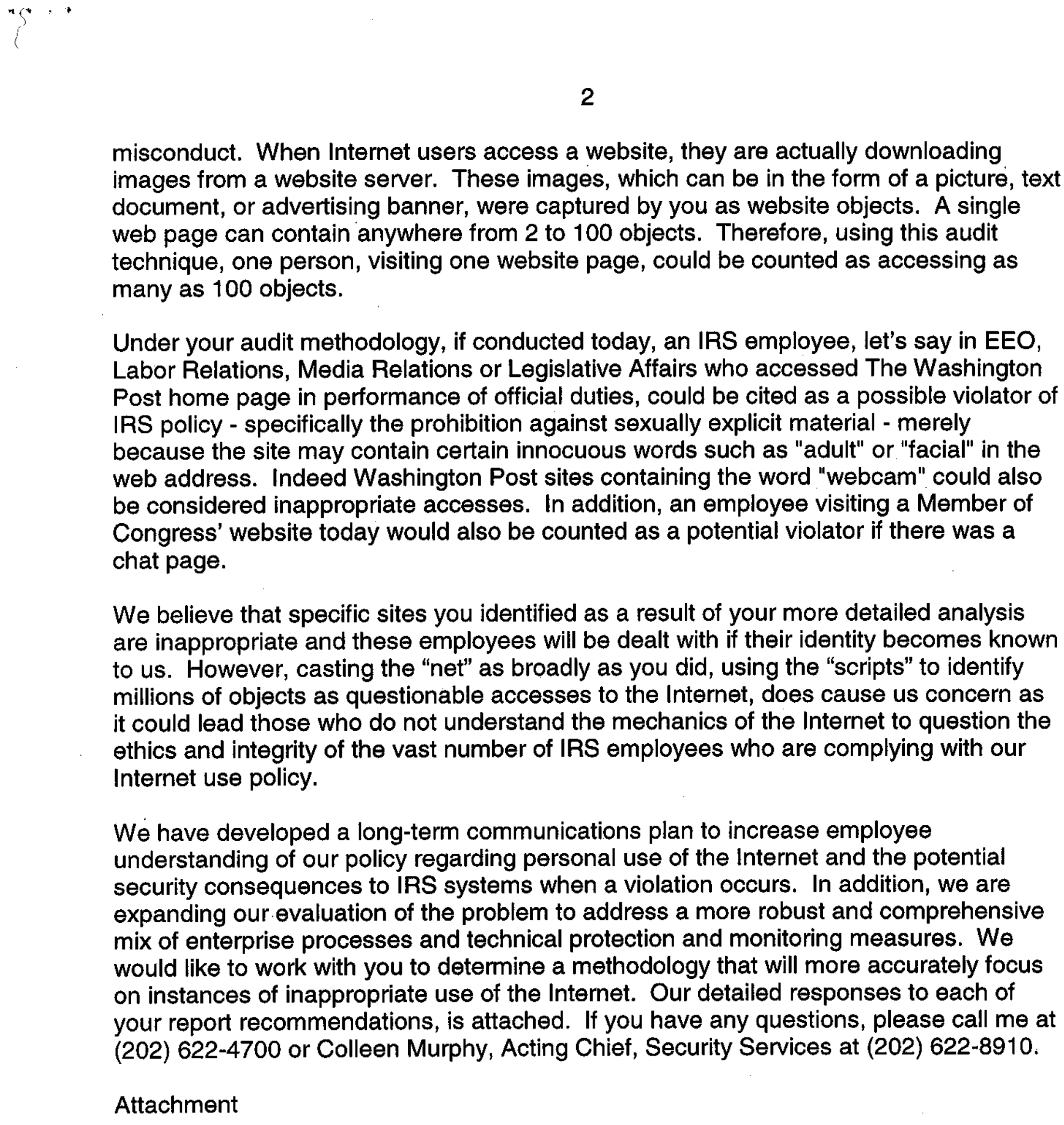
SUBJECT: Draft Audit Report – Inappropriate Personal Use of the Internet
Jeopardized the Security and Privacy of Taxpayer Data
(Audit #200320007)

The protection of taxpayer data is one of our most important responsibilities and I am taking immediate and aggressive steps to ensure employee compliance with our Internet policy. We appreciate your bringing this additional information and insight to this issue.

Using IRS systems to gain access to sexually explicit sites is offensive and wrong. Even one employee using the Internet for this purpose is one too many, and the IRS will not stand for it. We have terminated employees for these violations and others have resigned rather than face the embarrassment of termination. We continue to pursue any and all information at our disposal to address this problem and would appreciate any assistance you can provide that will enable us to identify employees engaged in this inappropriate behavior.

Your report also indicates that IRS "blocking" software was not totally effective. I find this unacceptable and I have directed the security staff to work with the vendor to improve our Internet architecture. Unfortunately, no one software solution can handle our consolidated Internet traffic volumes at this time. Therefore, we are investigating a more comprehensive suite of security solutions rather than relying exclusively on blocking.

Having acknowledged that the IRS has a problem with employees accessing inappropriate Internet sites, we recognize that your selective review of 283 sites out of a million accesses confirmed the existence of the problem. However, we are concerned about your count of potential violations. As noted in your report, website objects do not directly equate to websites accessed nor are they a fully reliable measurement of



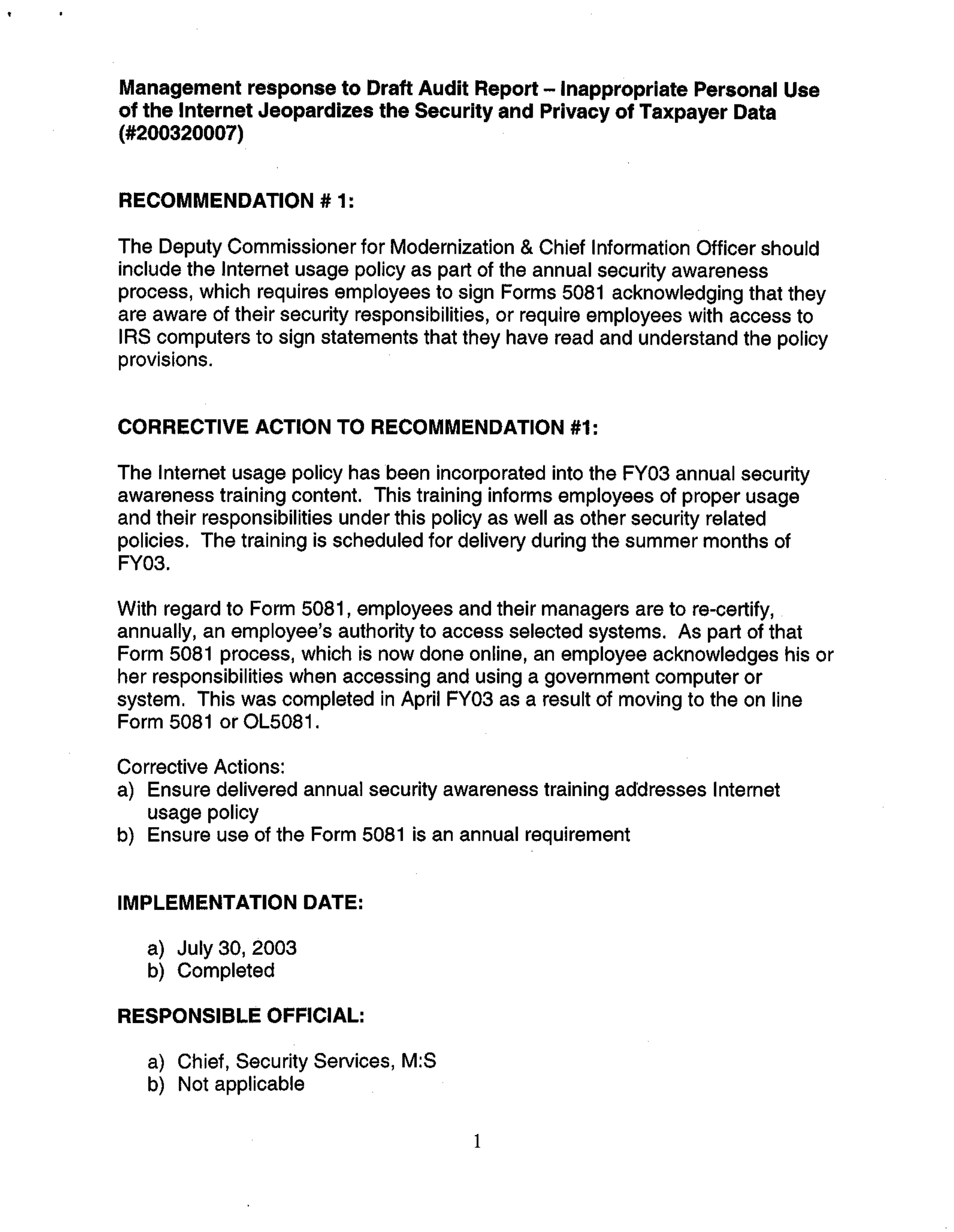
misconduct. When Internet users access a website, they are actually downloading images from a website server. These images, which can be in the form of a picture, text document, or advertising banner, were captured by you as website objects. A single web page can contain anywhere from 2 to 100 objects. Therefore, using this audit technique, one person, visiting one website page, could be counted as accessing as many as 100 objects.

Under your audit methodology, if conducted today, an IRS employee, let's say in EEO, Labor Relations, Media Relations or Legislative Affairs who accessed The Washington Post home page in performance of official duties, could be cited as a possible violator of IRS policy - specifically the prohibition against sexually explicit material - merely because the site may contain certain innocuous words such as "adult" or "facial" in the web address. Indeed Washington Post sites containing the word "webcam" could also be considered inappropriate accesses. In addition, an employee visiting a Member of Congress' website today would also be counted as a potential violator if there was a chat page.

We believe that specific sites you identified as a result of your more detailed analysis are inappropriate and these employees will be dealt with if their identity becomes known to us. However, casting the "net" as broadly as you did, using the "scripts" to identify millions of objects as questionable accesses to the Internet, does cause us concern as it could lead those who do not understand the mechanics of the Internet to question the ethics and integrity of the vast number of IRS employees who are complying with our Internet use policy.

We have developed a long-term communications plan to increase employee understanding of our policy regarding personal use of the Internet and the potential security consequences to IRS systems when a violation occurs. In addition, we are expanding our evaluation of the problem to address a more robust and comprehensive mix of enterprise processes and technical protection and monitoring measures. We would like to work with you to determine a methodology that will more accurately focus on instances of inappropriate use of the Internet. Our detailed responses to each of your report recommendations, is attached. If you have any questions, please call me at (202) 622-4700 or Colleen Murphy, Acting Chief, Security Services at (202) 622-8910.

Attachment



Management response to Draft Audit Report – Inappropriate Personal Use of the Internet Jeopardizes the Security and Privacy of Taxpayer Data (#200320007)

RECOMMENDATION # 1:

The Deputy Commissioner for Modernization & Chief Information Officer should include the Internet usage policy as part of the annual security awareness process, which requires employees to sign Forms 5081 acknowledging that they are aware of their security responsibilities, or require employees with access to IRS computers to sign statements that they have read and understand the policy provisions.

CORRECTIVE ACTION TO RECOMMENDATION #1:

The Internet usage policy has been incorporated into the FY03 annual security awareness training content. This training informs employees of proper usage and their responsibilities under this policy as well as other security related policies. The training is scheduled for delivery during the summer months of FY03.

With regard to Form 5081, employees and their managers are to re-certify, annually, an employee's authority to access selected systems. As part of that Form 5081 process, which is now done online, an employee acknowledges his or her responsibilities when accessing and using a government computer or system. This was completed in April FY03 as a result of moving to the on line Form 5081 or OL5081.

Corrective Actions:

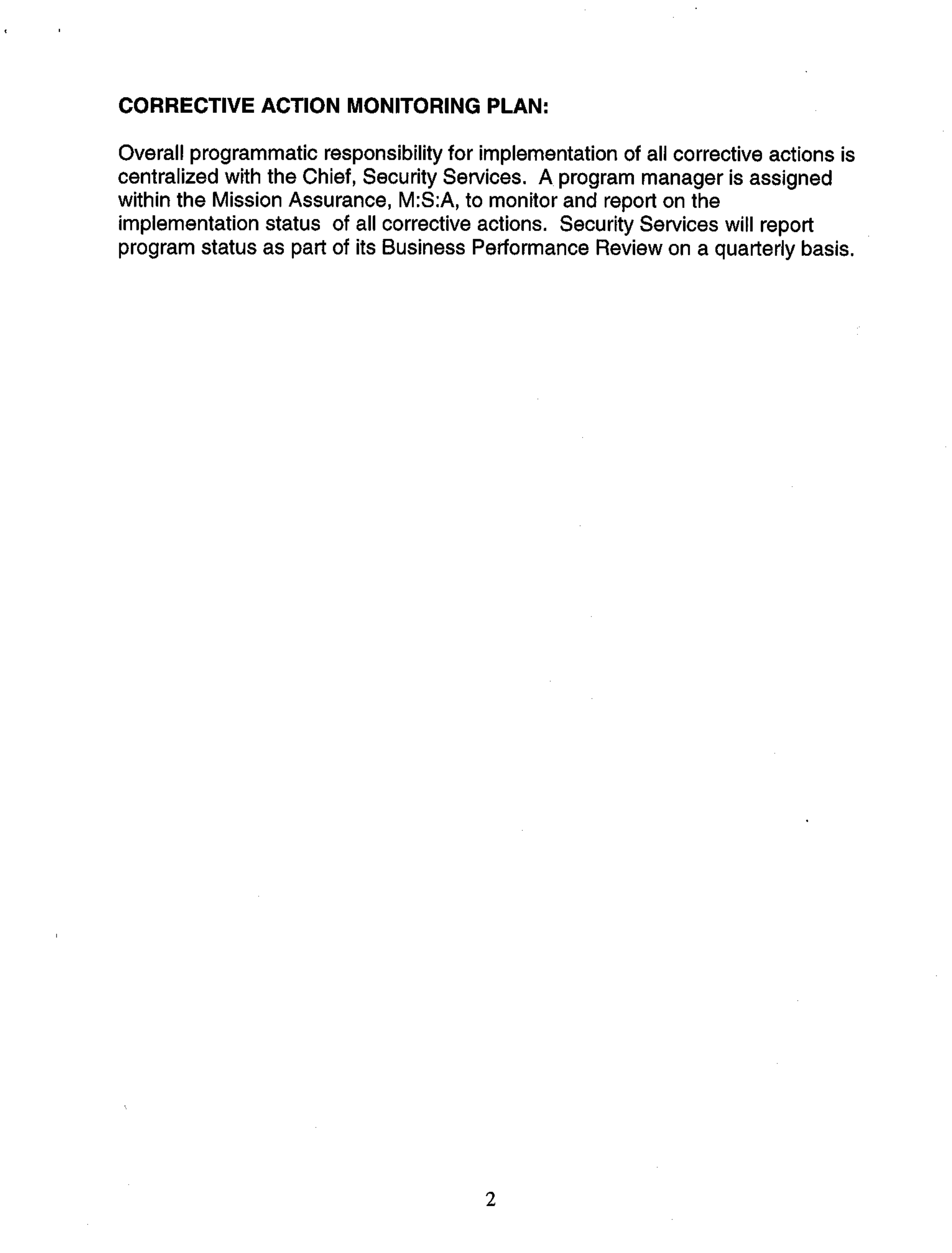
a) Ensure delivered annual security awareness training addresses Internet usage policy
b) Ensure use of the Form 5081 is an annual requirement

IMPLEMENTATION DATE:

a) July 30, 2003
b) Completed

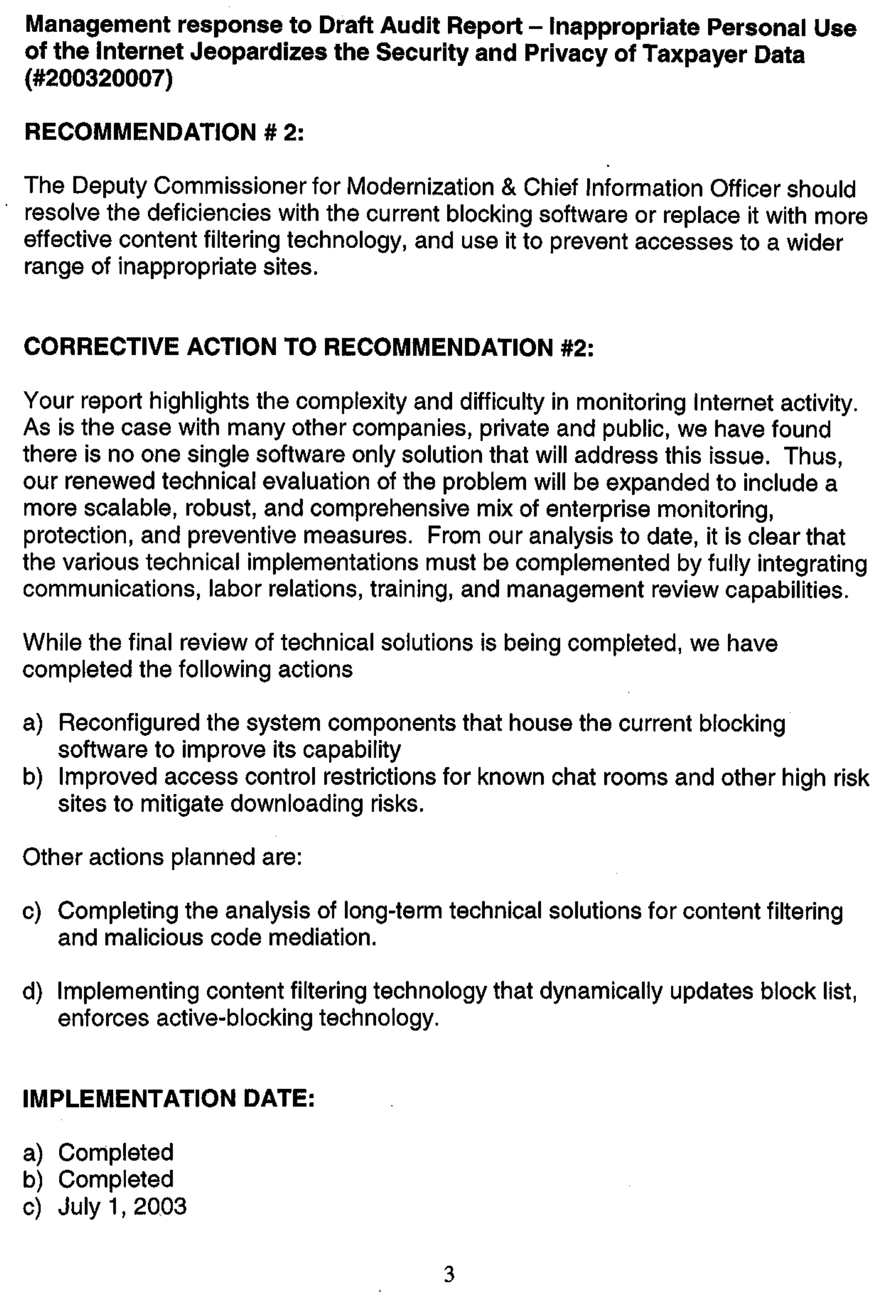
RESPONSIBLE OFFICIAL:

a) Chief, Security Services, M:S
b) Not applicable



CORRECTIVE ACTION MONITORING PLAN:

Overall programmatic responsibility for implementation of all corrective actions is centralized with the Chief, Security Services. A program manager is assigned within the Mission Assurance, M:S:A, to monitor and report on the implementation status of all corrective actions. Security Services will report program status as part of its Business Performance Review on a quarterly basis.



Management response to Draft Audit Report – Inappropriate Personal Use of the Internet Jeopardizes the Security and Privacy of Taxpayer Data (#200320007)

RECOMMENDATION # 2:

The Deputy Commissioner for Modernization & Chief Information Officer should resolve the deficiencies with the current blocking software or replace it with more effective content filtering technology, and use it to prevent accesses to a wider range of inappropriate sites.

CORRECTIVE ACTION TO RECOMMENDATION #2:

Your report highlights the complexity and difficulty in monitoring Internet activity. As is the case with many other companies, private and public, we have found there is no one single software only solution that will address this issue. Thus, our renewed technical evaluation of the problem will be expanded to include a more scalable, robust, and comprehensive mix of enterprise monitoring, protection, and preventive measures. From our analysis to date, it is clear that the various technical implementations must be complemented by fully integrating communications, labor relations, training, and management review capabilities.

While the final review of technical solutions is being completed, we have completed the following actions

a) Reconfigured the system components that house the current blocking software to improve its capability
b) Improved access control restrictions for known chat rooms and other high risk sites to mitigate downloading risks.

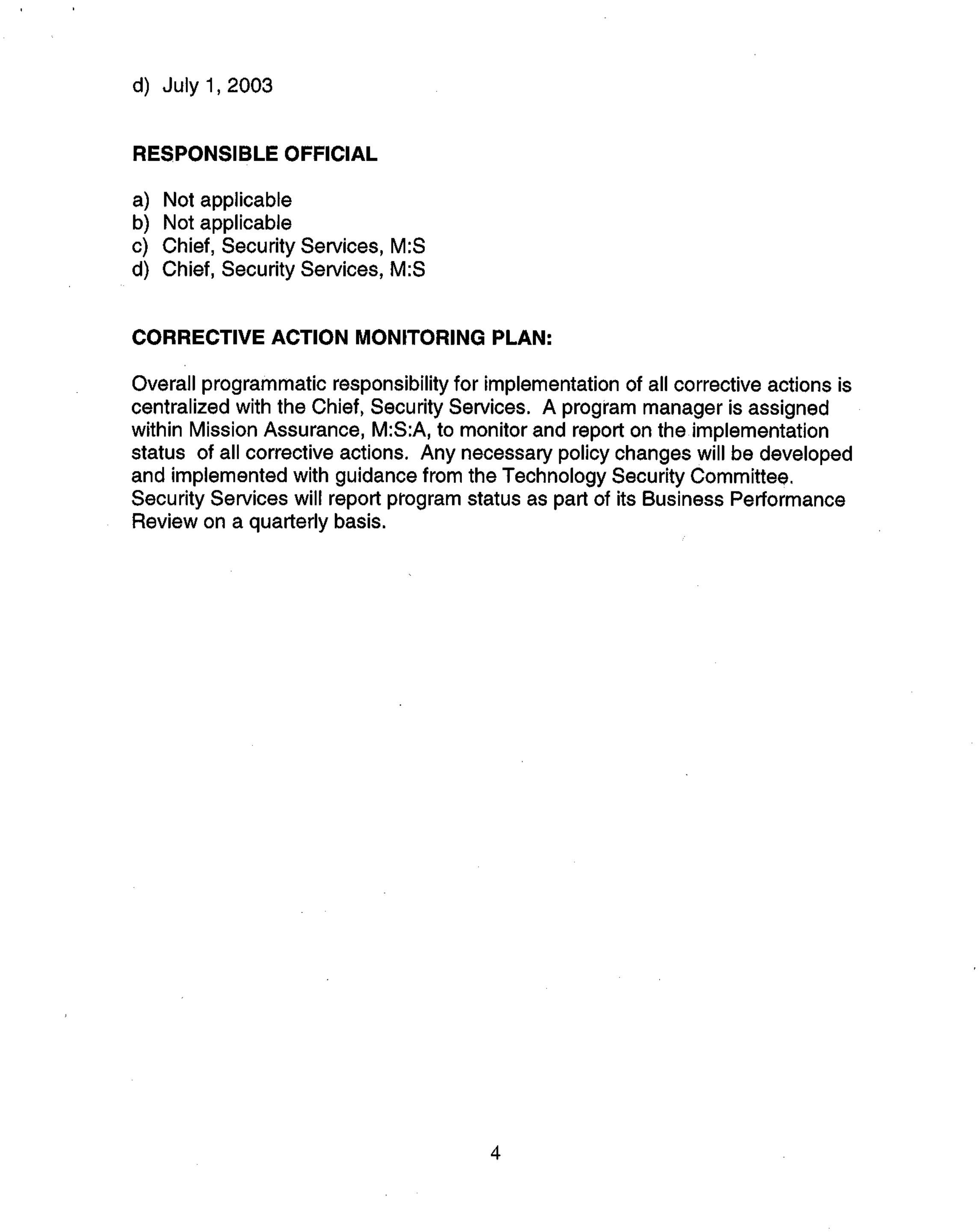
Other actions planned are:

c) Completing the analysis of long-term technical solutions for content filtering and malicious code mediation.

d) Implementing content filtering technology that dynamically updates block list, enforces active-blocking technology.

IMPLEMENTATION DATE:

a) Completed
b) Completed
c) July 1, 2003



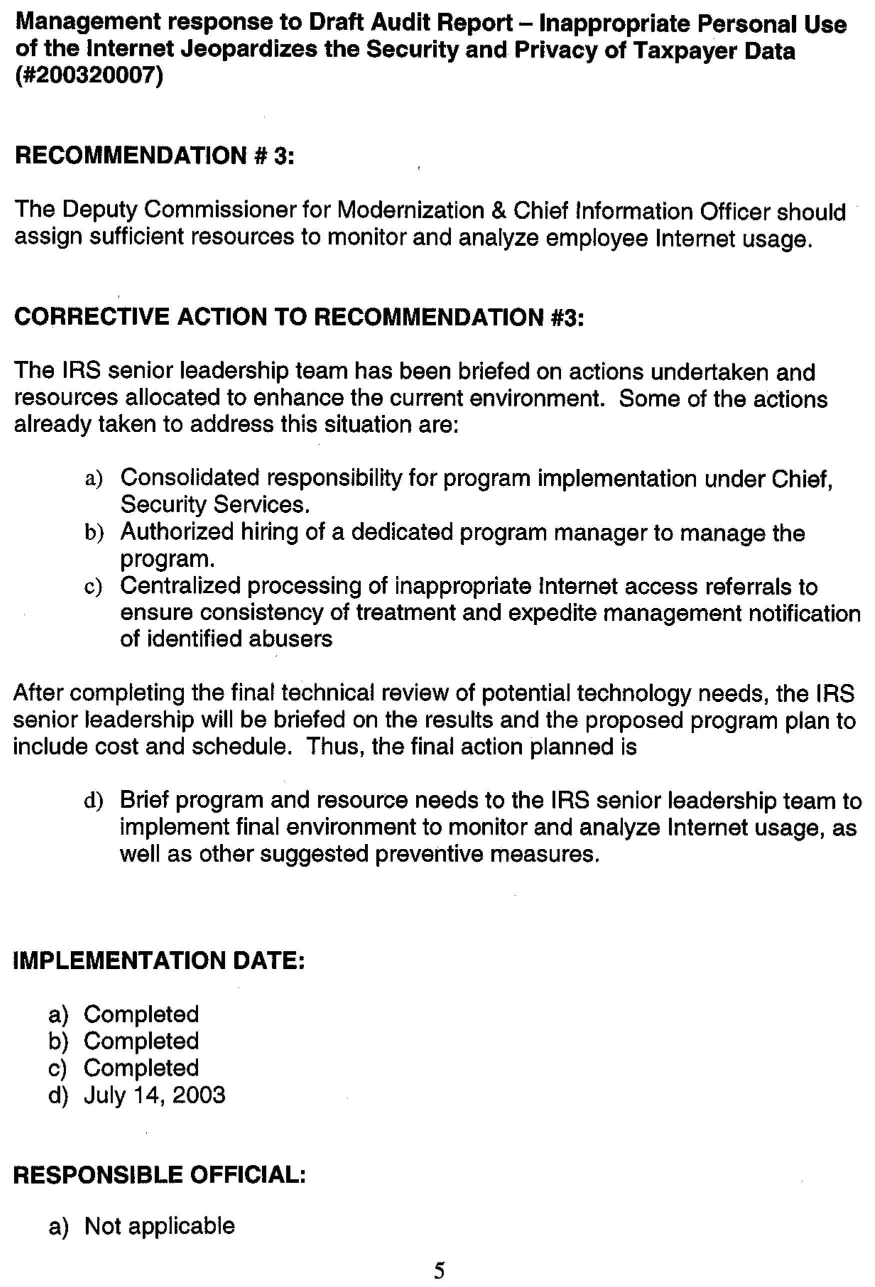
d) July 1, 2003

RESPONSIBLE OFFICIAL

a) Not applicable
b) Not applicable
c) Chief, Security Services, M:S
d) Chief, Security Services, M:S

CORRECTIVE ACTION MONITORING PLAN:

Overall programmatic responsibility for implementation of all corrective actions is centralized with the Chief, Security Services. A program manager is assigned within Mission Assurance, M:S:A, to monitor and report on the implementation status of all corrective actions. Any necessary policy changes will be developed and implemented with guidance from the Technology Security Committee. Security Services will report program status as part of its Business Performance Review on a quarterly basis.



Management response to Draft Audit Report – Inappropriate Personal Use of the Internet Jeopardizes the Security and Privacy of Taxpayer Data (#200320007)

RECOMMENDATION # 3:

The Deputy Commissioner for Modernization & Chief Information Officer should assign sufficient resources to monitor and analyze employee Internet usage.

CORRECTIVE ACTION TO RECOMMENDATION #3:

The IRS senior leadership team has been briefed on actions undertaken and resources allocated to enhance the current environment. Some of the actions already taken to address this situation are:

a) Consolidated responsibility for program implementation under Chief, Security Services.
b) Authorized hiring of a dedicated program manager to manage the program.
c) Centralized processing of inappropriate Internet access referrals to ensure consistency of treatment and expedite management notification of identified abusers

After completing the final technical review of potential technology needs, the IRS senior leadership will be briefed on the results and the proposed program plan to include cost and schedule. Thus, the final action planned is

d) Brief program and resource needs to the IRS senior leadership team to implement final environment to monitor and analyze Internet usage, as well as other suggested preventive measures.

IMPLEMENTATION DATE:

a) Completed
b) Completed
c) Completed
d) July 14, 2003

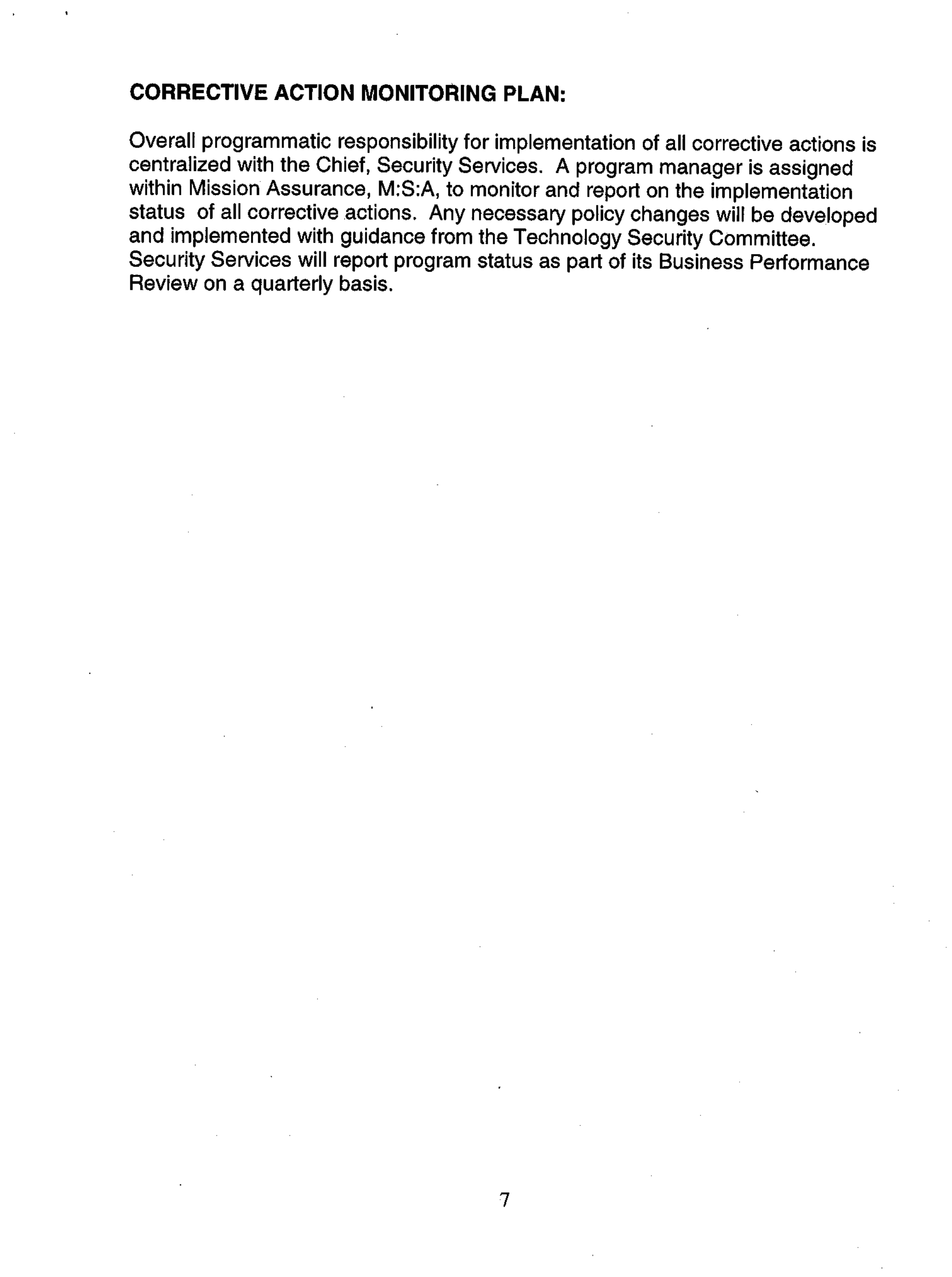
RESPONSIBLE OFFICIAL:

a) Not applicable

b) Not applicable

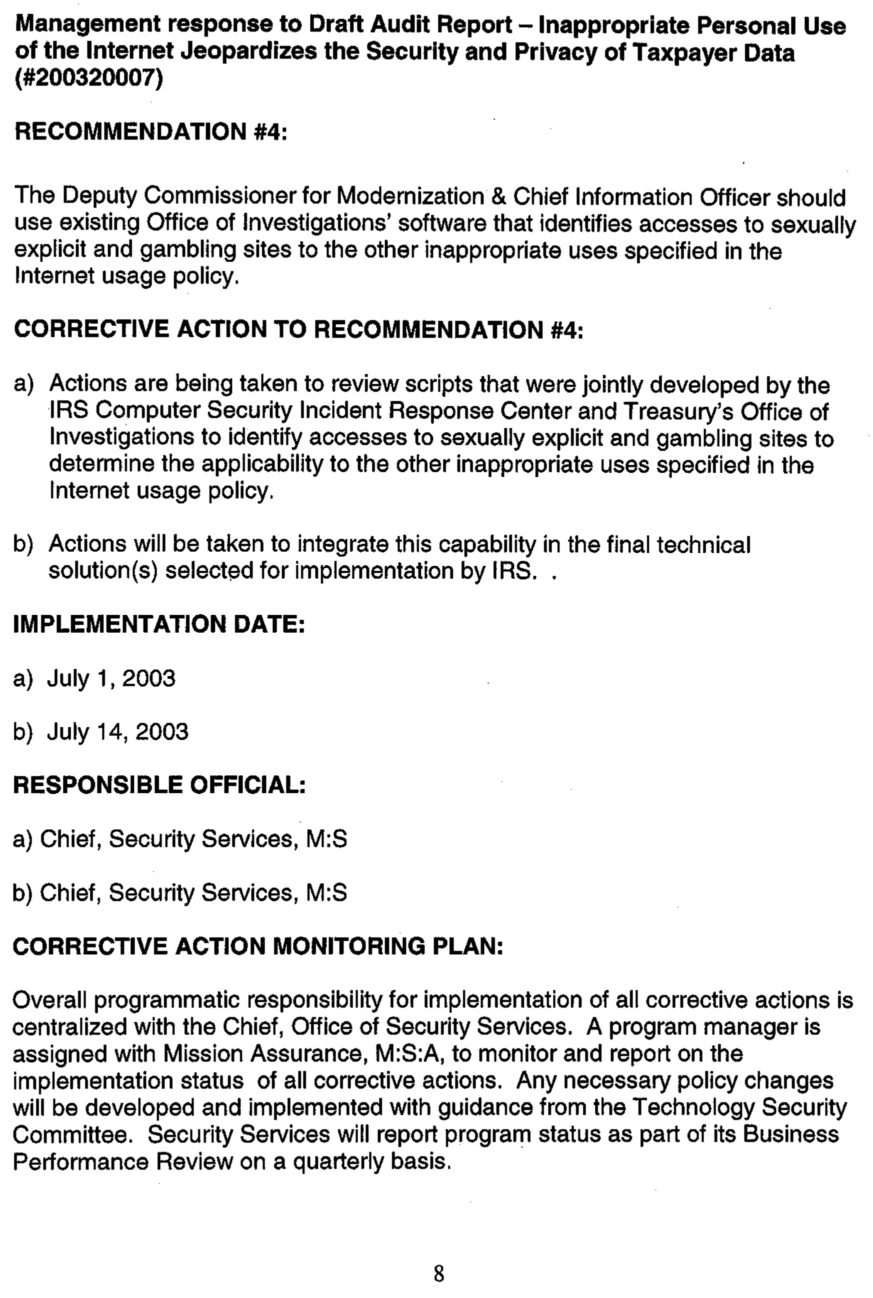
c) Not applicable

d) Deputy Commissioner for Modernization & Chief, information Officer, M



CORRECTIVE ACTION MONITORING PLAN:

Overall programmatic responsibility for implementation of all corrective actions is centralized with the Chief, Security Services. A program manager is assigned within Mission Assurance, M:S:A, to monitor and report on the implementation status of all corrective actions. Any necessary policy changes will be developed and implemented with guidance from the Technology Security Committee. Security Services will report program status as part of its Business Performance Review on a quarterly basis.



Management response to Draft Audit Report – Inappropriate Personal Use of the Internet Jeopardizes the Security and Privacy of Taxpayer Data (#200320007)

RECOMMENDATION #4:

The Deputy Commissioner for Modernization & Chief Information Officer should use existing Office of Investigations' software that identifies accesses to sexually explicit and gambling sites to the other inappropriate uses specified in the Internet usage policy.

CORRECTIVE ACTION TO RECOMMENDATION #4:

a) Actions are being taken to review scripts that were jointly developed by the IRS Computer Security Incident Response Center and Treasury's Office of Investigations to identify accesses to sexually explicit and gambling sites to determine the applicability to the other inappropriate uses specified in the Internet usage policy.

b) Actions will be taken to integrate this capability in the final technical solution(s) selected for implementation by IRS. .

IMPLEMENTATION DATE:

a) July 1, 2003

b) July 14, 2003

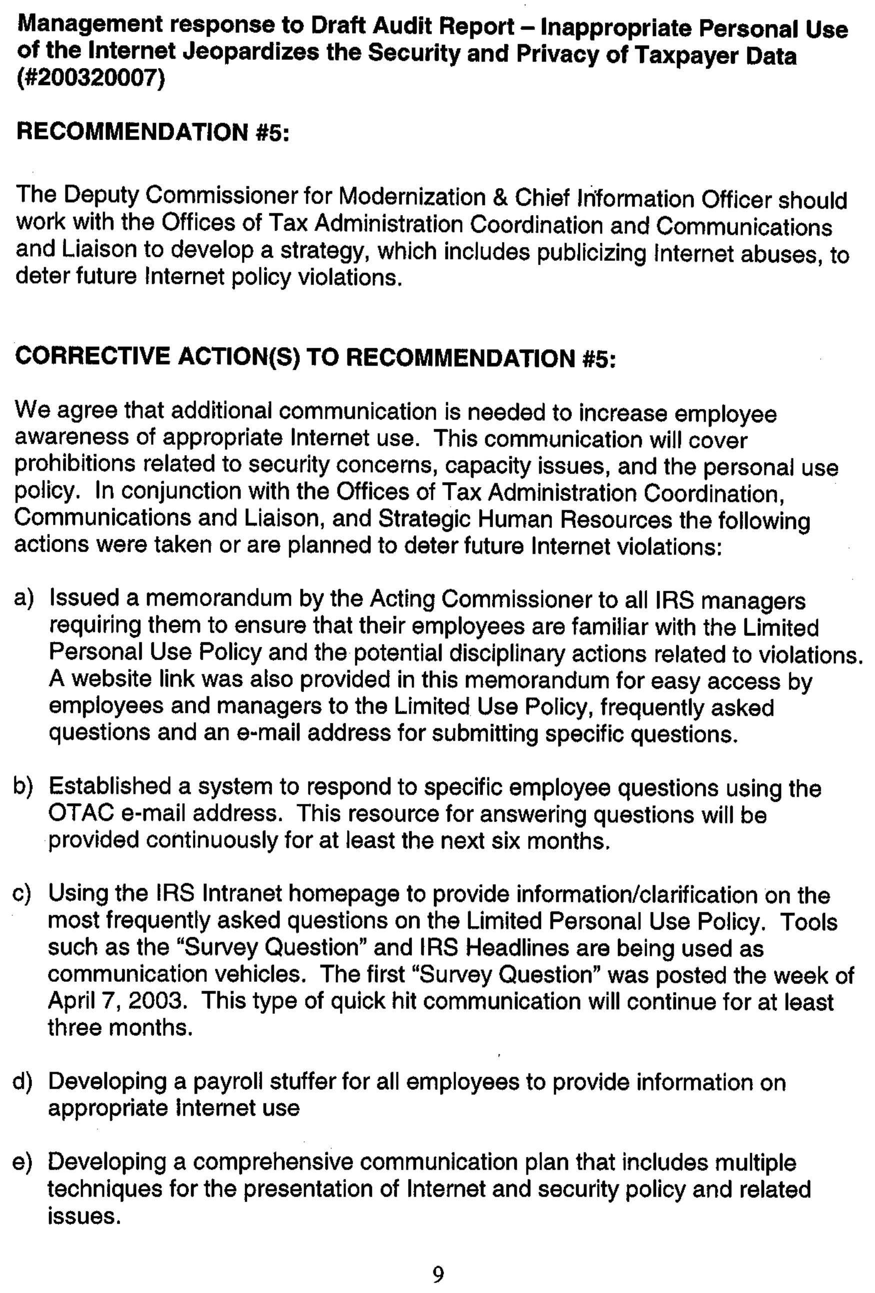
RESPONSIBLE OFFICIAL:

a) Chief, Security Services, M:S

b) Chief, Security Services, M:S

CORRECTIVE ACTION MONITORING PLAN:

Overall programmatic responsibility for implementation of all corrective actions is centralized with the Chief, Office of Security Services. A program manager is assigned with Mission Assurance, M:S:A, to monitor and report on the implementation status of all corrective actions. Any necessary policy changes will be developed and implemented with guidance from the Technology Security Committee. Security Services will report program status as part of its Business Performance Review on a quarterly basis.



Management response to Draft Audit Report – Inappropriate Personal Use of the Internet Jeopardizes the Security and Privacy of Taxpayer Data (#200320007)

RECOMMENDATION #5:

The Deputy Commissioner for Modernization & Chief Information Officer should work with the Offices of Tax Administration Coordination and Communications and Liaison to develop a strategy, which includes publicizing Internet abuses, to deter future Internet policy violations.

CORRECTIVE ACTION(S) TO RECOMMENDATION #5:

We agree that additional communication is needed to increase employee awareness of appropriate Internet use. This communication will cover prohibitions related to security concerns, capacity issues, and the personal use policy. In conjunction with the Offices of Tax Administration Coordination, Communications and Liaison, and Strategic Human Resources the following actions were taken or are planned to deter future Internet violations:

a) Issued a memorandum by the Acting Commissioner to all IRS managers requiring them to ensure that their employees are familiar with the Limited Personal Use Policy and the potential disciplinary actions related to violations. A website link was also provided in this memorandum for easy access by employees and managers to the Limited Use Policy, frequently asked questions and an e-mail address for submitting specific questions.

b) Established a system to respond to specific employee questions using the OTAC e-mail address. This resource for answering questions will be provided continuously for at least the next six months.

c) Using the IRS Intranet homepage to provide information/clarification on the most frequently asked questions on the Limited Personal Use Policy. Tools such as the "Survey Question" and IRS Headlines are being used as communication vehicles. The first "Survey Question" was posted the week of April 7, 2003. This type of quick hit communication will continue for at least three months.

d) Developing a payroll stuffer for all employees to provide information on appropriate Internet use

e) Developing a comprehensive communication plan that includes multiple techniques for the presentation of Internet and security policy and related issues.

f) Providing periodic communication to all employees of information on disciplinary actions resulting from Internet violations.

IMPLEMENTATION DATE:

a) Completed - March 28, 2003

b) Completed

c) August 1, 2003

d) August 1, 2003

e) June 1, 2003

f) October 1, 2003

RESPONSIBLE OFFICIAL(S):

a) Director, Tax Administration Coordination, N:ADC:T

b) Director, Tax Administration Coordination, N:ADC:T

c) Director, Communication and Liaison, CL
Responsible Partners:
Director, Tax Administration Coordination, N:ADC:T
Chief, Security Services, M:S

d) Director, Communication and Liaison, CL
Responsible Partner:
Chief, Security Services, M:S

d) Director, Communications and Liaison, CL
Responsible Partners:
Chief, Communications Policy and Programs, M:C
Director, Tax Administration Coordination, N:ADC:T

e) Director, Communications and Liaison, CL
Responsible Partner:
Director, Office of Workforce Relations, N:ADC:H:R

CORRECTIVE ACTION MONITORING PLAN:

Ongoing Internet monitoring by Security Services as well as the evaluation of cases referred to Labor Relations for possible disciplinary action will provide the basis for determining the success of recommended communication efforts and the need for additional actions. Security Services and Labor Relations will report on their findings related to Internet violations as part of their Business Performance Reviews and also alert the Director, Communication and Liaison if additional communication actions are needed.